IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	**)**	
	)	
v.	**)**	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	**)**	
Defendant	**)**	

DEFENDANT'S MOTION FOR ISSUANCE OF A SUBPOENA *DUCES TECUM* PURSUANT TO RULE 17(c) AND MEMORANDUM IN SUPPORT THEREOF

Okello Chatrie, through counsel, respectfully moves this Court to enter an Order directing that a subpoena *duces tecum* be issued to Google LLC ("Google") pursuant to Rule 17(c) of the Federal Rules of Criminal Procedure, and that Google be required to provide the responsive documents and things prior to the anticipated hearing on Mr. Chatrie's *Motion to Suppress Evidence Obtained from a "Geofence" General Warrant*, ECF No. 29, in order to allow the parties sufficient time to review the information and prepare for that hearing. The grounds for this Motion, including the subpoena to be issued, are set forth below.

INTRODUCTION

On October 29, 2019, Mr. Chatrie filed two related motions. The first was a motion to suppress evidence obtained from the Google "geofence" warrant, as well as its fruits. *See* ECF No. 29. The second was motion for discovery concerning the use of Google's "Sensorvault" data in this case. *See* ECF No. 28. Because Mr. Chatrie's motion to suppress presents constitutional questions of first impression, and because so little is publicly known about the underlying technology and processes at issue, Mr. Chatrie has consistently maintained that access to further

information is necessary and material to preparing his defense, and to his suppression motion in particular.

While the government has provided some of the information requested by Mr. Chatrie in ECF No. 28, it also asserted that other defense requests concerning Google's practices and policies "relate to documents and or information not in the United States' possession, custody, or control." ECF No. 38 at 1. Instead, on October 19, 2019, the government averred that the materials the defense seeks "remain in the possession, custody, and control of Google." *Id.* at 8. The government then further noted that Rule 17(c) provides Mr. Chatrie with compulsory process through which to order the production of documents from Google. *Id.* at 8 n.6.

On December 3, 2019, Google notified the parties of its intent to file an *amicus* brief in support of neither party. On December 9, 2019, Mr. Chatrie filed his reply to the government's response to the discovery motion, arguing that Google was a part of the government's investigative team with respect to the use of Google's location data in this case. *See* ECF No. 49 at 2-4. As a result, Mr. Chatrie further argued that pursuant to Federal Rule of Criminal Procedure 16 and *Brady v. Maryland*, 373 U.S. 83, 87 (1963), the onus is on the government to either obtain the requested information from Google, or abandon its reliance on the geofence data altogether. *Id.* at 4-5.

On December 20, 2019, Google filed its *amicus* brief in support of neither party. *See* ECF No. 59-1. In its brief, Google proffered some new facts that strongly support Mr. Chatrie's motion to suppress, such as the fact that complying with *any* geofence warrant entails searching *every user* for whom Google has location history data. However, as Mr. Chatrie noted in his response, the information Google provided is also incomplete. *See* ECF No. 72 at 1-2. It does not address, for example, defense requests for information "on the categories of data Google collected, stored, and

provided to law enforcement" or the "specific inputs and algorithms used to produce the responsive Location History data in this case." *Id*. It also raised additional questions about whether users voluntarily and intentionally convey their location information to Google. *Id*. at 5-9.

On January 21, 2020, the Court held a hearing on the outstanding discovery issues in this case. During that hearing, Mr. Chatrie introduced expert testimony concerning the relevance of the missing information apparently in Google's possession as well as additional information about the Location History feature raised by Google's *amicus* brief. The Court questioned the defense as to why counsel had not sought a Rule 17(c) subpoena to obtain this this information directly from Google. The Court also indicated that doing so would not prejudice Mr. Chatrie's pending discovery requests under Rule 16 and *Brady*. *See* 1/21/20 Tr. at 185.

Consequently, Mr. Chatrie now moves this Court to issue a subpoena directing Google to produce the following documents and things pursuant to Rule 17(c):

1. Google policies, procedures, instructions, or manuals concerning geofence warrants, including:
    a. a description of the different types of location data that Google collects and maintains (e.g., "Location History," "Google Location Services," "Web and App Activity" data);
    b. which data type(s) Google searches in response to geofence warrants, and the rationale, if any, for limiting the type(s) of data searched;
    c. the process for "anonymizing" and re-identifying the user location data provided to law enforcement;

2. Statistics identifying the percentage of Google users who had enabled Location History, Google Location Services, and Web & App Activity, separately or in combination, during 2019;

3. Records indicating the physical location of the Wi-Fi access points used to estimate the location of users deemed responsive to the first step of the geofence warrant process;

4. The algorithm Google used to estimate the location of users deemed responsive to the first step of the geofence warrant process, including the error rate and any validation studies.

As discussed below, this information is relevant to and admissible in a pre-trial hearing on Mr. Chatrie's motion to suppress the geofence warrant. The defense has been unable to procure it from the government or elsewhere,[1] but it is nonetheless essential to Mr. Chatrie's proper preparation for the suppression hearing. This is no fishing expedition. Rather, Mr. Chatrie seeks specific information in Google's possession that goes to the heart of his suppression argument that the geofence warrant entailed a Fourth Amendment search that was so overbroad and lacking particularity as to render it an unconstitutional general warrant.

ARGUMENT

1. Legal Standard for Issuance of Rule 17(c) Subpoenas

Rule 17 of the Federal Rules of Criminal Procedure governs the issuance of subpoenas in criminal cases. Subsection (c) provides, in relevant part:

> A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

Fed. R. Crim. P. 17(c)(1). "Rule 17(c) implements the Sixth Amendment guarantee that an accused have compulsory process to secure evidence in his favor." *In re Martin Marietta Corp.*, 856 F.2d 619, 621 (4th Cir. 1988); *see also United States v. Llanez-Garcia*, 735 F.3d 483, 493 (6th Cir. 2013) (observing that Rule 17(c) "implements a criminal defendant's constitutional right 'to have compulsory process for obtaining witnesses in his favor' by providing a means to subpoena witnesses and documents for a trial or a hearing. U.S. Const. amend. VI[.]") (citing 2 Charles Alan Wright et al., Federal Practice and Procedure § 272 (4th ed.) ("Rule 17 is not limited to subpoenas for the trial" and observing that a subpoena may be issued for a preliminary examination, a grand

[1] Should Google have any concerns about the sensitivity of this information, the parties can surely come to an agreement on the terms of an adequate protective order.

jury investigation, a deposition, a determination of a factual issue raised by a pre-trial motion, or a post-trial motion).

In *United States v. Nixon*, the Supreme Court set forth the standards for issuing a Rule 17(c) subpoena. 418 U.S. 683, 699-700 (1974). Adopting the test devised by Judge Weinfeld in *United States v. Iozia*, pre-trial production of evidence is appropriate where the moving party shows:

> (1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general 'fishing expedition.'

Id. (citing *United States v. Iozia*, 13 F.R.D. 335, 338 (SDNY 1952)). The *Nixon* Court further distilled this test to three factors: (1) relevancy; (2) admissibility; (3) specificity. *Id.* at 700.

It is well-settled that Rule 17(c) is not to be used as a broad discovery tool, nor as a means to gather materials for impeachment purposes only. *See, e.g.*, *id.* at 700-01; *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951); *United Sates v. Beckford*, 964 F.Supp. 1010, 1032 (E.D.Va. 1997). Furthermore, the decision whether to issue a Rule 17(c) subpoena and require the documents be produced pre-trial rests with the sound discretion of the district court. *Nixon*, 418 U.S. at 702; *Beckford*, 964 F.Supp. at 1021 n.9. And while Rule 17(c) does not explicitly require a party to make a motion to the court prior to issuance of a subpoena, doing so "is an orderly and desirable procedure and one frequently followed" in this jurisdiction. *Beckford*, 964 F.Supp. at 1021.

Finally, although most cases involving Rule 17(c) concern production prior to "trial," the Court's authority under Rule 17(c) relates to a judicial "proceeding," *see* Fed. R. Crim. P. 17(a), which includes pre-trial hearings. *See* 2 Charles Alan Wright et al., Federal Practice and Procedure

§ 272 (4th ed.). In this case, the documents and things relate to a pre-trial hearing on Mr. Chatrie's motion to suppress the evidence produced by Google as a result of the geofence warrant, as well as all of the fruits thereof. *See* ECF No. 29. The Court has already indicated that it intends to hold such a hearing, the outcome of which may be dispositive in this case. Mr. Chatrie therefore seeks pre-hearing access the documents in question in order to allow the parties sufficient time to review them and prepare for that hearing, consistent with Rule 17(c). *See* Fed. R. Crim. P. 17(c)(1) (permitting courts to require production pre-trial or "before they are to be offered in evidence").

2. The Information Sought from Google is Relevant.

All of the information Mr. Chatrie seeks from Google relates to at least one of three aspects of his suppression claim: breadth, particularity, or voluntariness.

Request (1) concerns Google's process for collecting and maintaining user location data of all types, as well as Google's process for searching that data and producing ostensibly "anonymized" records pursuant to a geofence warrant. Documents describing these processes bear on the breadth and particularity of the geofence warrant, as well as the degree of voluntariness involved in conveying the underlying location data to Google. Whereas the warrant requires Google to produce location data for "each type" of Google account inside the 150-meter geofence, *see* ECF No. 54-1 at 4, 9, Google proffered in its *amicus* brief that it limited its initial search to so-called "Location History" data only, meaning that it did not search location data generated as a result of "Google Location Services" or "Web & App Activity." *See* ECF No. 59-1 at 12. Google provides no support for this assertion and no rationale for why it would restrict the search in a manner contrary to the plain language of the warrant. This request is particularly relevant given the testimony at the January 21, 2020, hearing that in other cases, Google specifies its source of the location data. 1/21/20 Tr. at 29-31.

From a Fourth Amendment perspective, it is essential to know the true reach of the search at issue. Google collects and stores user location data in at least three ways: via Location History, Google Location Services, and/or Web & App Activity. By searching Location History data only, Google appears to limit the scope of the initial search and lower the total number of users affected, compared to a search of all three types of data. For purposes of particularity, it is also critical to know whether and why Google may have limited its search in this manner, as granting such discretion to non-judicial officers is likely to violate the Fourth Amendment's particularity requirement. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356). Additionally, the facts will speak to whether the data searched by Google was conveyed by users voluntarily. As the government argues, the degree of voluntariness involved reflects on whether Google users have a reasonable expectation of privacy in their location data. *See* ECF No. 41 at 10. Google maintains that users must opt-in[2] to Location History tracking through a multi-step process, *see* ECF No. 59-1 at 7-8, whereas Google Location Services and Web & App Activity are enabled by default. But if the geofence search did include either of these two types of location data, then the voluntariness calculation would shift further in Mr. Chatrie's favor.

Finally, request (1) seeks documentation explaining how Google provides "anonymized" data to law enforcement in the initial two phases of the geofence warrant process. The defense believes that the warrant misrepresented the intrusiveness of these first two steps by describing the data to be produced as "anonymized." In fact, as the defense demonstrated through expert testimony on January 21, 2020, Google's use of pseudonyms in place of user IDs is little more

[2] Mr. Chatrie does not concede that the "opt-in" procedure that Google has devised for location history is in fact truly knowing and voluntary for the vast majority of users.

than a legal fig leaf. 1/21/20 Tr. at 73-92. The unique user paths delineated by the Google location coordinates may be sufficient, without more, to ascertain the likely identity of the user. *See also* ECF No. 68 at 3-5. Furthermore, it appears there may be a direct and predictable relationship between the pseudonyms assigned by Google and the true device IDs that have been supposedly anonymized. If true, this omission would further undermine the government's contention that the data initially produced to law enforcement raised minimal privacy concerns, as it may have effectively granted law enforcement access to more identifiable information than the warrant appears to authorize. This fact would be directly relevant the warrant's breadth and particularity.

Request (2) relates to many of the same fundamental issues as request (1), seeking the percentage of Google users who have Location History enabled in 2019, as well as similar statistics for Google Location Services, and Web & App Activity. Together with the requested policies and procedures describing which types of location data Google searches, these statistics will allow the defense to determine the total number of Google users who were searched during the initial phase of the geofence warrant process. The answer will likely confirm the warrant's unprecedented breadth and lack of particularity. The figures will also permit the parties to determine how many users have enabled which different types of location tracking, a fact that will further inform the voluntariness determination.

Request (3) seeks records indicating the physical location of the Wi-Fi access points used to estimate the location of users deemed responsive to the first step of the geofence warrant process. This information relates directly to the breadth and particularity of the warrant, as it appears that the search swept up users who were well outside of the 150-meter geofence due to the way in which Google "estimates" location based on Wi-Fi data. Google asserts that the location data points it produced to law enforcement were not "historical fact[s]" but merely "probabilistic

estimate[s]" with a "margin of error" that "reflects Google confidence in the reported coordinates." *See* ECF No. 59-1 at 10, *id*. n.7, 13 n.8, 20 n.12. Indeed, this margin of error tends to be very large for coordinates based on Wi-Fi data, which comprise 88% of the data points in the initial warrant return. *See* ECF No. 68 Ex. A. Google does not, however, explain how these estimates, margins of error, or confidence values were calculated, leaving the defense with no way to verify their accuracy. The defense therefore seeks records indicating the location of the Wi-Fi access points used to estimate which users were within the 150-meter radius prescribed in the geofence warrant.

As Mr. Chatrie has previously explained, a Wi-Fi access point can be a "router, switch, Ethernet cable hub, or some other device that creates a wireless local area network." *See* ECF No. 49 at 7. Mobile devices "see" the access points in their vicinity and their relative signal strength. *Id.* The devices report this information to Google, which then uses the information to estimate the device's location with the aid of an algorithm. *Id.* The trouble is that Wi-Fi networks have their own ranges, which do not conveniently stop at walls or property lines—or at 150 meters from the Call Federal Credit Union. Instead, they have an average outdoor range of 300 feet, *see* ECF No. 72 at 15-16, meaning that a Wi-Fi access point close to edge of the 150-meter geofence would likely be "seen" by devices far beyond it. And as a result, Google may "estimate" that a device is within the geofence when it was not. Indeed, the defense elicited expert testimony on January 21, 2020, that at least one of the three users whose information was de-anonymized in the final step of the warrant process here ("Mr. Green"), was likely never inside the geofence at all, but simply driving down a road next to it on his way home from a nearby hospital. 1/21/20 Tr. at 82. Access to information about the location of the relevant Wi-Fi access points in this case will permit the defense to determine how many devices Google may have been falsely identified as within the 150-meter geofence. The government presented no information to the issuing magistrate about the

true scope of the geofence warrant or the likelihood of ensnaring people outside of its perimeter. These facts, however, go directly to Mr. Chatrie's overbreadth and particularity arguments, as he maintains that the scope of the search was impermissibly broad and afforded too much discretion to law enforcement to determine whose data would be produced and ultimately de-anonymized.

For the same reasons, request (4) seeks the algorithm Google used to estimate the location of users deemed responsive to the first step of the geofence warrant process, including the error rate and any validation studies. Like the location of the Wi-Fi access points, understanding Google's algorithm—i.e., its mathematical method of estimating device locations based on available inputs, like Wi-Fi data—and its shortcomings is critical to assessing how broad the search here really was, as well as the discretion involved in determining whose data would be produced to law enforcement. The algorithm will allow the defense to determine how many devices may have been falsely identified as having been within the 150-meter geofence. It will also allow the defense to verify the proffered error rates and confidence values to the same end. Like the Wi-Fi access point locations, the algorithm relates directly to Mr. Chatrie's overbreadth and particularity arguments. If Google provided the government with "estimates" instead of "facts," then the defense deserves to know how Google is came up with those estimates, especially if Google's process effectively expands the scope of the search in a way unknown to the magistrate who signed the warrant.

In sum, all of the information the defense seeks from Google is relevant to demonstrating that the geofence warrant in this case was a flawed Fourth Amendment search, profoundly overbroad and lacking in particularity. The requested documents and things go to the scope of the initial search, both in terms of the total number of users whose data was searched by Google, as well as the number of individuals whose information was initially provided by Google to law

enforcement. The lack of clarity about which data would be searched and what law enforcement would receive is likewise relevant to Mr. Chatrie's particularity argument. Indeed, it appears that the government presented no information to the issuing magistrate concerning the effective scope of the geofence search, the likelihood of sweeping up devices outside of the 150-meter radius, or the identifiable nature of the supposedly "anonymized" location data produced to law enforcement. All of these points are relevant to Mr. Chatrie's suppression motion, but without the information he seeks from Google, he will be unable to present them at the pre-trial suppression hearing.

3. The Information Sought from Google is Admissible.

All of the information sought from Google here would be admissible in a pre-trial hearing on Mr. Chatrie's motion to suppress the geofence data obtained from Google and its fruits. The applicable standard for admissibility under Rule 17(c) is the same standard that would apply if the defense were to introduce the evidence at the pre-trial suppression hearing, which is not the same as the standard for admissibility at trial.[3] In an evidentiary hearing on a motion to suppress, relaxed rules of evidence apply. Under Federal Rule of Evidence 104(a), "[p]reliminary questions concerning … the admissibility of evidence shall be determined by the court, [which] is not bound by the rules of evidence except with respect to privileges." Just as the out-of-court statements of a confidential informant might properly support a finding of probable cause, *see United States v. Matlock*, 415 U.S. 164, 172–73 (1974), so too may a judge receive evidence in support of suppression that may not be admissible before a jury. A judge will rightly "give it such weight as his [or her] judgment and experience counsel." *Id.*

[3] As discussed above, Rule 17(c) clearly contemplates such pre-trial proceedings, permitting courts to require production either "before trial" or pre-trial or "before they are to be offered in evidence." Fed. R. Crim. P. 17(c)(1).

Furthermore, as the Supreme Court suggested in *Nixon*, a lower evidentiary standard may also apply when a subpoena is directed to a third-party rather than the government. *See* 418 U.S. at 699 n.12. This is because the "evidentiary" requirement has developed mainly in cases in which defendants have sought pre-trial disclosure from the government under Rule 17(c), as opposed to Rule 16 or *Brady*. Prior to *Nixon*, the leading case on Rule 17(c) was *Bowman Dairy v. United States*, which involved a subpoena seeking documents the government had obtained through confidential informants. 341 U.S. 214, 218 (1951). *Bowman* recognized a defendant's right to obtain such materials under 17(c) if "any part of them are not put in evidence by the Government." *Id.* at 219. Otherwise, the Court reasoned, the government could "exclude from the reach of process of the defendant any material that had been used before the grand jury or could be used at trial." *Id.* at 221. In short, the *Bowman* Court viewed Rule 17(c) as a way to obtain materials for trial that the defense likely learned about from the discovery provided by the government under Rule 16. *Id.* at 219. *Bowman*'s requirement that these materials be "evidentiary" was a way of distinguishing between the type of material subject to broad discovery under Rule 16 and demands for producing specific documents under Rule 17(c). *Id.* at 219-220. Thus, the Court found one part of the subpoena in *Bowman* unenforceable because it contained "catch-all" demand amounted to a "fishing expedition." *Id.* at 221. Critically, however, the Court assumed that the recipient of the subpoena would be the government, which has independent discovery obligations under Rule 16.

In the wake of *Bowman*, courts began to adopt the four-part formulation first articulated a year later in *Iozia*, 13 F.R.D. at 338. *See supra* at 5. Like *Bowman*, *Iozia* involved a subpoena to the government seeking documents that had been voluntarily provided to the government by a third party. While the court found that aspect of the subpoena to be enforceable, it also found that demands for 11 years-worth of files from investigating agencies were too broad and had "every

appearance of a fishing expedition" aimed at uncovering impeachment evidence. *Iozia*, 13 F.R.D. at 340. Nonetheless, the court recognized the government's Rule 16 obligations and noted that the defense would have prior access to any relevant impeachment evidence for any person called to testify at trial. *Id*.

It was against this background that the *Nixon* Court adopted the *Iozia* factors. The Court was therefore careful to note that, with respect to the "evidentiary" prong in particular, the situation in *Nixon* was unlike *Bowman Dairy* or *Iozia*. *See* 418 U.S. at 699 n.12. These facts presented "the more unusual situation … where the subpoena, rather than being directed to the government by defendants, issues to what, as a practical matter, is a third party." *Id*. This was significant because the party seeking the subpoena in *Nixon* could not first avail itself of discovery under Rule 16, unlike the defendants in *Bowman Dairy* and *Iozia*. The Court therefore left the door open to the possibility that the evidentiary requirement may not apply with "full vigor" when the subpoena is directed to a third party. *Id*. In sum, the somewhat stringent standard derived from *Bowman Dairy* and *Iozia* was crafted with subpoenas between the prosecution and defense in mind, not access to information held by a third party like Google. With respect to third parties, the text of Rule 17(c) simply codifies the traditional right of the prosecution or the defense to seek evidence for trial by a subpoena *duces tecum*.

Thus, when a criminal defendant subpoenas a third-party such as Google in preparation for suppression hearing, *Nixon*'s admissibility requirement does not apply with full force. Instead, Mr. Chatrie "need only show that the request is (1) reasonable, construed as "material to the defense," and (2) not unduly oppressive for the producing party to respond." *United States v. Tucker*, 249 F.R.D. 58, 66 (S.D.N.Y. 2008), *as amended* (Feb. 20, 2008). Under such relaxed rules of evidence, all the documents and things requested by the subpoena here are most certainly "admissible," as

they are highly relevant and material to demonstrating the overbreadth and lack of particularity in the geofence warrant, as well as to the voluntariness with which users create and store their geolocation information with Google. Moreover, production of the requested materials would not be "unduly oppressive" for Google. Producing policies and statistics pursuant to requests (1) and (2) would appear to require minimal effort, as would producing the locations of the Wi-Fi access points pursuant to request (3). Likewise, the act of producing the location-estimating algorithm pursuant to request (4) is straightforward and would not require significant time or effort.

4. The Information Sought from Google is Specific.

Mr. Chatrie has identified the information he seeks from Google with sufficient specificity. In this context, specificity embodies both the "good faith" and "fishing expedition" concepts that the *Nixon* Court imported from *Iozia*. *See United States v. King*, 194 F.R.D. 569, 573 (E.D. Va. 2000).

Although Mr. Chatrie does not know the precise title or format in which Google explains its policies and procedures for responding to geofence warrants, the defense elicited expert testimony on January 21, 2020, that Google is likely to have such documents, which it now seeks pursuant to request (1). 1/21/20 Tr. at 92-93. Furthermore, such internal policies are not publicly available and the defense has been unable to obtain this information from the government. By contrast, they would be easily identifiable and familiar to Google, which by its own count, saw a 1,500% increase in geofence requests in 2018. *See* ECF No. 59-1 at 3. Likewise, the court heard expert testimony that Google maintains statistics on the number of devices with Location History enabled, as they do for Google Location Services and Web & App Activity as well. 1/21/20 Tr. At 59-60. Request (2) further specified that the defense seeks this information for 2018 only.

Request (3) seeks the location of the Wi-Fi access points that Google identified as the "source" of the location data provided to law enforcement. Google used this information in order to estimate users' locations and determine who was likely inside the 150-meter geofence, as a defense expert testified on January 21, 2020. 1/21/20 Tr. at 64-68. Google therefore has it and is aware of precisely which access points are at issue here, even though the defense is not. Similarly, request (4) seeks the algorithm Google used to calculate users' locations based on the Wi-Fi data. To use a simple analogy, the algorithm is like a math formula and the Wi-Fi access points are variables. Whereas Google provided the government with spreadsheets full of answers and confidence values, the defense asking Google to show its work. In short, Google is surely aware of the algorithm and Wi-Fi data that the defense seeks here because Google used this information to respond to the geofence warrant.

Mr. Chatrie has therefore described the documents and things he seeks with sufficient specificity. This is no fishing expedition, but a focused request for information from Google that is not otherwise available to the defense. Mr. Chatrie seeks these materials in good faith and maintains that they are highly relevant and material to his suppression argument.

CONCLUSION

For the foregoing reasons, Mr. Chatrie respectfully requests that this Court enter an Order pursuant to Rule 17(c) directing that a subpoena *duces tecum* be issued to Google for the documents and things described in requests (1)-(4), *supra* at 3. Mr. Chatrie further requests that Google be required to provide the responsive documents and things prior to the anticipated suppression hearing and with sufficient time for the parties to review and analyze them beforehand.

Respectfully submitted,

OKELLO T. CHATRIE

By: _____/s/_____

Michael W. Price
NY Bar No. 4771697 (pro hac vice)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on February 4, 2020, I filed the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to all counsel of record.

_____/s/_____

Laura Koenig
Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org